Cyber Security: Modern-Day Warfare and Practical Countermeasures

Overview

The game has changed. Today's threat landscape is continually changing, the attack types and motivations are more organized and sophisticated than ever before, and are routinely escalating in organization, complexity, and sponsorship. We are now seeing Nation-States and other nefarious bad actors targeting critical and governmental organizations at rates never before seen, with specific motivations and intent behind the attacks.

To make matters worse, the FUD (Fear, Uncertainty, and Doubt) factor being promulgated by Security vendors, with their own motivations, is also increasingly difficult to decipher. These two very real characteristics of cyber security in the 21st Century make it difficult to effectively understand how best to manage risk, as no organization has unlimited funding to address cyber security.

This paper is based upon a summary of the joint presentation between the Colorado Statewide Internet Portal Authority (SIPA), and Level 3 Communications' Information Security experts. The aim of this paper is to provide a glimpse into perspectives shared from the government sector, based on a limited group of respondents to a survey, coupled with how the market perceives Risk, and then to offer practical guidance for managing risk in the 21st Century.

We dub this "Modern-Day Warfare," as we see cyber security to be the new, and for the foreseeable future, very real front in a battlefield which knows no borders. The Truth about Statistics and Surveys

Before we jump into a few results of our local survey, and also analyze some external surveys, Statistics, and "Intelligence," we'd like to briefly touch upon Interpretation of the Results. Statistics require analysis and interpretation, and numbers alone often do not tell the whole story. Context is critical to significance, even when discussing "factual evidence." Surveys are subjective opinion that can be misleading based on the following elements:

- Response options

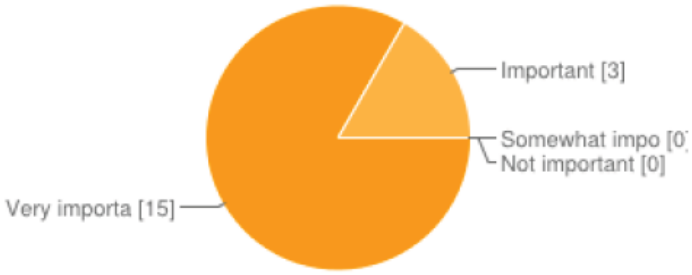
- Context of the question
- Role of respondents
- Result and Evidence contradictions

Surveys are most useful when compared to evidence, and used to help understand the gap between reality and belief. Because of these important considerations, we provide several different data points, from different perspectives, to try and outline a more clear picture of "what the real story is."

Local Survey Results

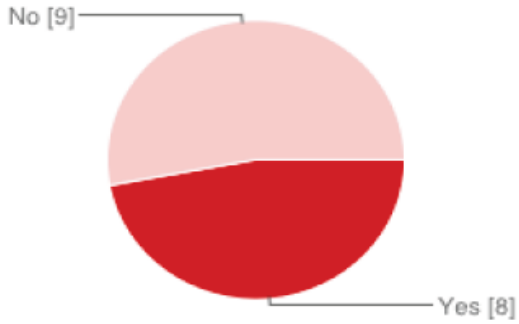
SIPA and Level 3 Communications jointly created a survey, and polled responses from many Colorado Government entities, across all sectors. This included the very small and localized organizations, as well as the very large and distributed. We present a few of those findings in this section, and encourage you to ponder how your organization might also respond, as these are salient points which should give pause for serious consideration.

How important is cyber security to your organization?



Very important	15	83%
Important	3	17%
Somewhat important	0	0%
Not important	0	0%

Does your organization have a single person responsible for cyber security?

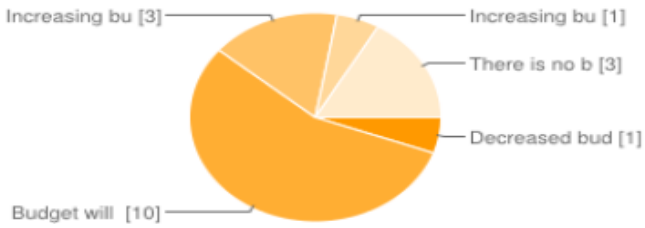


Yes	8	47%
No	9	53%

These two data points are very interesting, when put into "context," or comparison with each other. The vast majority of respondents believe cyber security is very important, yet the majority of respondents do not have a single person responsible for cyber security. We certainly understand budget constraints, but our point here is perception vs. reality. The majority of respondents *believe* it's

very important, yet the majority has not been able to *justify* and *define* a single person responsible for cyber security in their organization.

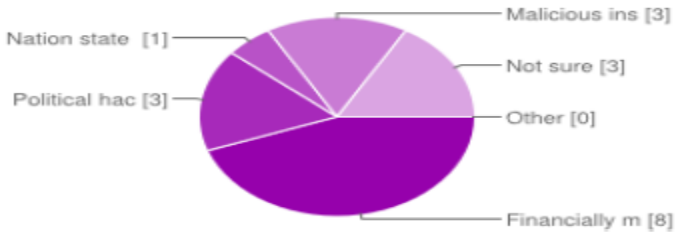
What will happen to your information security budget in the next year compared to the last year?



Decreased budget	**1**	6%
Budget will remain the same	**10**	56%
Increasing budget by less than 15 percent	**3**	17%
Increasing budget by more than 15 percent	**1**	6%
There is no budget	**3**	17%

Indeed, with extremely tight budgets, it's very difficult for government organizations to justify staffing a security professional, but in our view, this is a challenge which must be overcome. If your systems are connected to the Internet, it's truly only a matter of time before you can expect to either be breached, or worse yet, be *notified* of a breach by a Third Party. The critical question actually becomes: How can you afford *not* to have a single person responsible for Cyber Security?

Who do you see as the greatest information security threat to your organization?



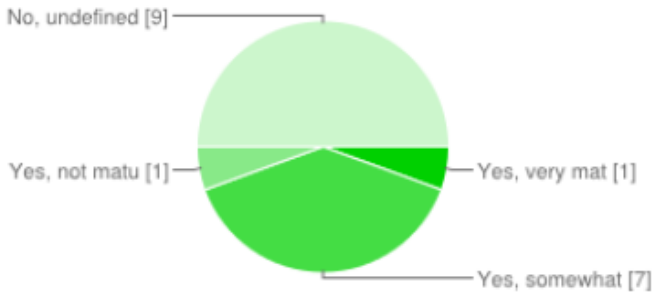
Financially motivated external hackers	**8**	44%
Political hacktivists	**3**	17%
Nation state sponsored hackers	**1**	6%
Malicious insiders	**3**	17%
Not sure	**3**	17%
Other	**0**	0%

This particular response is very interesting. Keep in mind, this was a Survey of Government Organizations, and yet, the vast *minority* perceives Nation-State and Politically motivated attackers to be among the least significant Threat. While it is true that financially-motivated external hackers do pose a significant threat, from our perspective, particularly for Government agencies, we also believe

significant weight should be given to the threats posed by Nation-state and politically motivated hackers.

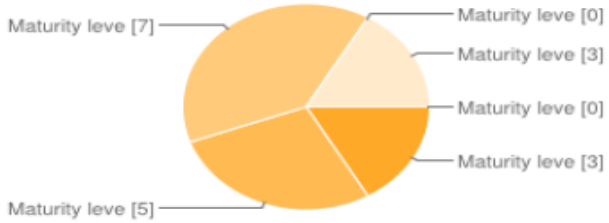
Finally, we wrap up this section on our local Survey with just a few more points about proactive, responsible, risk-informed decision-making, and effective risk management. When we speak of "risk-informed," we mean that an organization has an Information Security Program, with current routines, policies, and procedures in place to support that Program – in order to fully understand risks (not just vulnerabilities), *and thereby enabled to make informed decisions about where to spend the limited security budget.*

Do you have an ISMS (Information Security Management System in place and how mature is that system?



Yes, very mature	**1**	6%
Yes, somewhat mature	**7**	39%
Yes, not mature	**1**	6%
No, undefined	**9**	50%

Which of the following best describes the documented security policies within your organization?



Maturity level 5: Comprehensive, enforceable, enforced, measured and reported	**0**	0%
Maturity level 4: Comprehensive, enforceable, mostly enforced, somewhat measured and reported	**3**	17%
Maturity level 3: Mostly complete, mostly enforceable, somewhat enforced, not measured or reported	**5**	28%
Maturity level 2: Mostly complete, somewhat enforceable, lightly enforced, not measured or reported	**7**	39%
Maturity level 1: Rudimentary, somewhat enforceable, not enforced, not measured or reported	**0**	0%
Maturity level 0: non-existent	**3**	17%

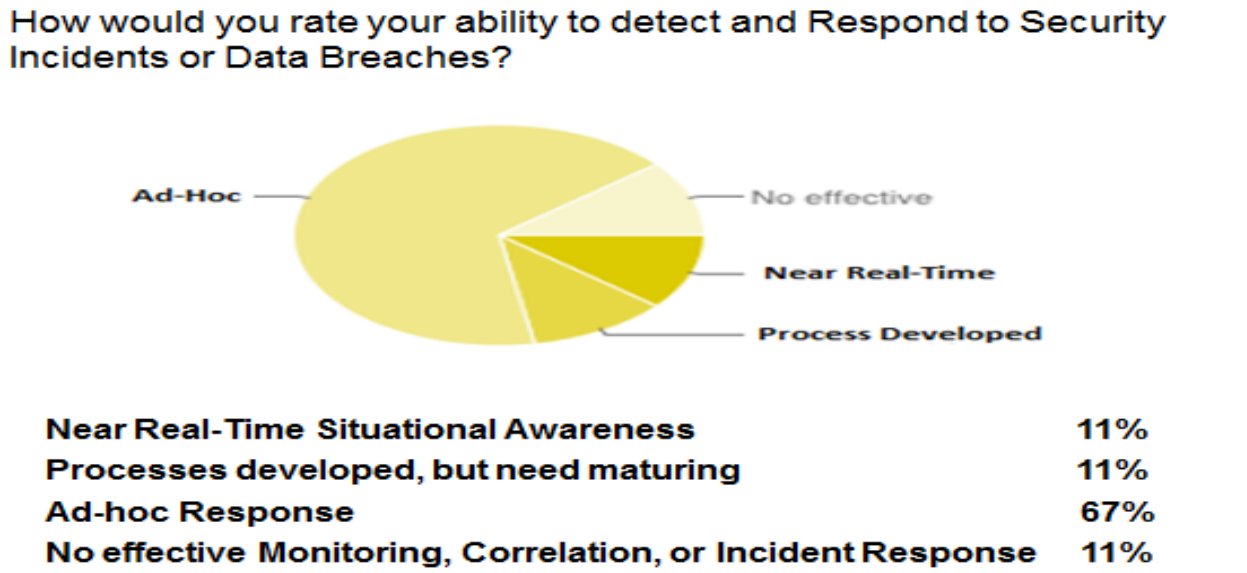
Without an effective Information Security Management System, supported by current, relevant, *enforceable* Security Policies, it is very difficult to make informed risk management decisions. How are you able to determine where best your limited budget should be expended without these basic cornerstones? Effective risk management, especially the type required to have a fighting chance on this modern day battlefield, *requires* that there is a comprehensive Program, supported by current and

enforceable policies, procedures, and appropriate technologies. Regular testing (at least annually) by an objective Third Party should be performed, in order to provide a feedback loop into assumptions about the effectiveness of the Risk Management Program.

It is our strong opinion that an objective Third Party Assessment, performed on a regular basis, is a fundamentally important, nay vital, aspect of any Risk Management Program. It will validate, or refute, assumptions made about an organization's overall risk posture, and provide keen insight into one's security posture. Because such reliance should be put on these Assessments, and value derived from them, they should be performed by experts. We strongly dissuade organizations from simply selecting the "lowest cost provider" who is going to "perform an audit." Audits are necessary and required, but should be perceived differently than a security assessment, and most certainly different from a penetration test.

The latter two require highly specialized skillsets, and we see all too often providers that use low-cost individuals, coupled with automated testing toolkits, providing "Security Assessments" and "Penetration Tests" for organizations – and giving those organizations a false sense of security. This is the one "point-in-time" where an organization is able to get significant value for "Security Spend," if performed and utilized properly. It is also the same "point-in-time" to achieve a false sense of security by reliance on low-cost providers utilizing weak skillsets and automated tools.

While we have further data points illustrating the majority of government organizations do not regularly undergo Third Party Assessments, and penetration tests, we'll end this section with one final data point that supremely accents the need for a comprehensive Program, supported by appropriate policies, procedures, and technologies.



Near Real-Time Situational Awareness	**11%**
Processes developed, but need maturing	**11%**
Ad-hoc Response	**67%**
No effective Monitoring, Correlation, or Incident Response	**11%**

It is encouraging to see that a small set of organizations believe they have "Near Real-Time Situational Awareness." We do have some questions about that perspective, and would also like to see that validated with a Third Party Assessment! But more importantly, the vast majority of respondents have

an Ad-hoc ability to Detect and Respond to Security Incidents and Data Breaches. This speaks volumes to the focus in the right areas of risk management. We acknowledge it is a non-trivial task to proactively glean "Intelligent Awareness" from disparate data points, log systems, and "even-correlation" systems. But the greater questions remain: What toolsets exist, how often are they tuned and tested, and what policies and procedures are in place to detect and respond? How do you classify and contain security incidents and data breaches? Do you know where all of your sensitive data is, and are you certain about all the connected systems with "authorized" access to that critical data? How often are *those* systems tested for vulnerabilities, access permissions, and other key considerations?

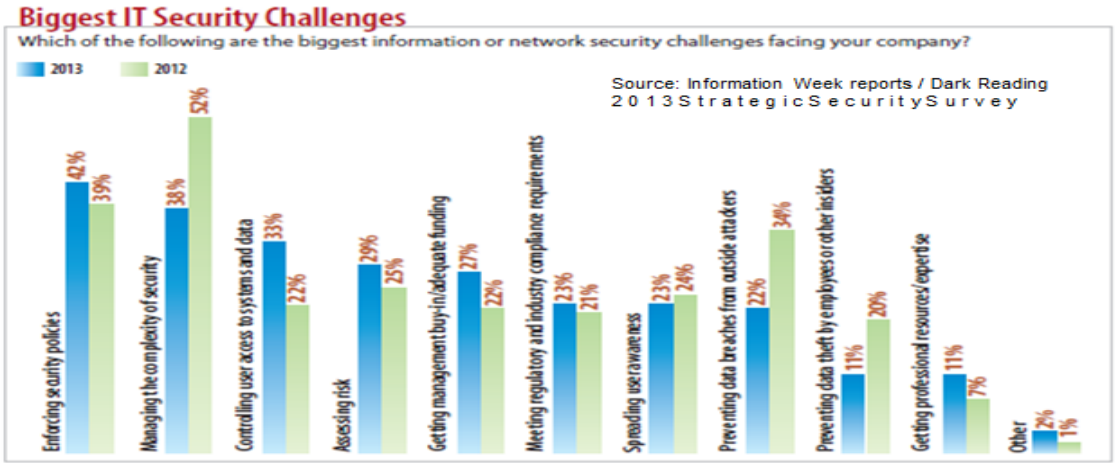
External Viewpoints

Now we turn our attention to a few external perspectives to establish a bit more context around the local survey responses. These data points also include Surveys and Statistics, with the same inherent limitations identified earlier, yet they offer additional insight into the "Problem Space," and help us stabilize the "Perception vs. Reality" situation before moving into final recommendations.

Darkreading.com, an excellent source of useful insight around many topics within the realm of information security, published its own survey. This comprised a much larger pool of respondents, and also offers interesting perspective on how the larger information security community perceives risk.

What Worries Your Peers in the Enterprise Market?

- **1,029** respondents are recognizing the value of awareness
- **13%** saying they're more vulnerable than last year
- **73%** see mobility as a threat
- **75%** admit they may be ignorant of a Breach



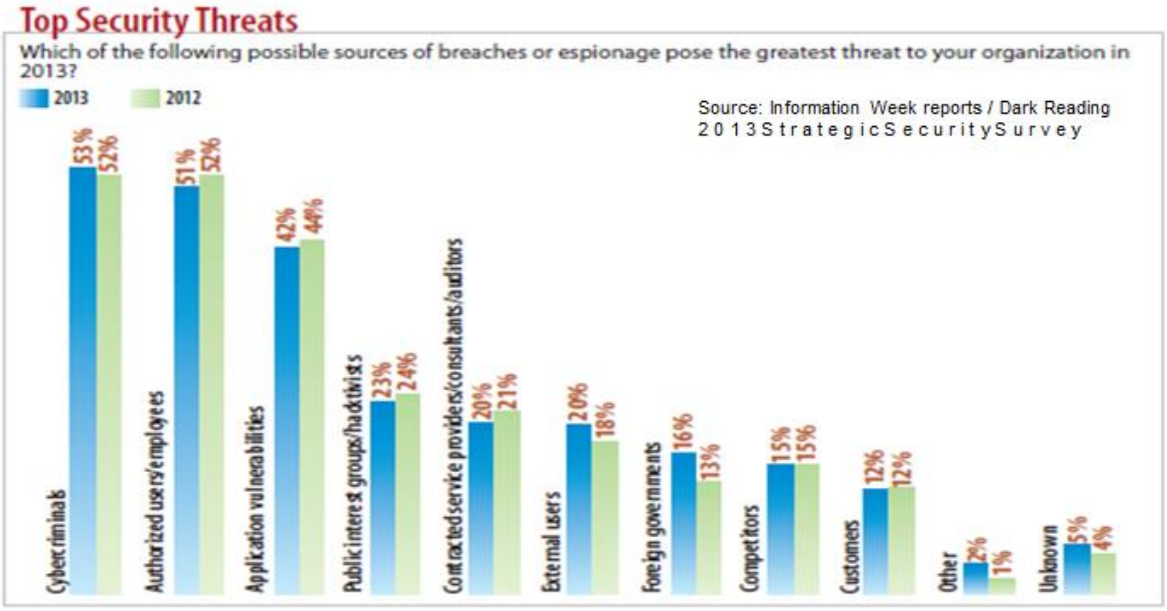
One of the most interesting elements of this survey response is the concern about managing the complexity of security. All too often we see organizations getting wrapped up in a "more tools" perspective, possibly pushed by vendors with specific game plans to further expand their dominance in the marketplace. We aren't discounting the importance of a solid, effective toolset – they are a critical element to a comprehensive risk management program. But tools (i.e. technologies) aren't the only answer; they must be equally supported by proper policies, training, and procedures.

It is our opinion that tools have supplanted their value in the risk management ecosystem, *precisely because they have become the primary focus of Risk Managers.* Without proper training, personnel, procedures, and effective policies, all of which should be tested and refined on a continual basis, the tools will lead to great concern about "managing the complexity of security." Again, we are not saying that tools don't serve a valuable purpose, they most certainly do – but they are only one element, and should not be the only focus, of IT Risk Managers, for an effective Risk Management Program.

Shifting our focus to perceived threats identified by this survey, we find an interesting disparity between these responses, and our own local survey – with respect to Hacktivism. We certainly find them to be an increasing threat, with a solid toolset at their disposal, and greater motivation.

What is the Source of the Threat?

- Criminals, Internal Users, Application Vulnerabilities, and Hacktivists still ranked in the top 4.



Keeping in mind the inherent bias mentioned earlier, the definition of "Cybercriminals" certainly is a large net to cast! But our experience has shown this is a fairly decent classification of both organized groups, and specific motivations. For instance, we see Distributed Denial of Service (DDoS) attacks increasing in sophistication, intent, and scale – at alarming rates. In 2012, the largest attack we saw across the Internet, targeting Financial Organizations, was approximately 80 Gigabits/second (Gbps) in size. This year, the most recent attack size we've seen is 160 Gbps, and over 120 million packets per second. Those attacks are designed to take sites and systems offline.

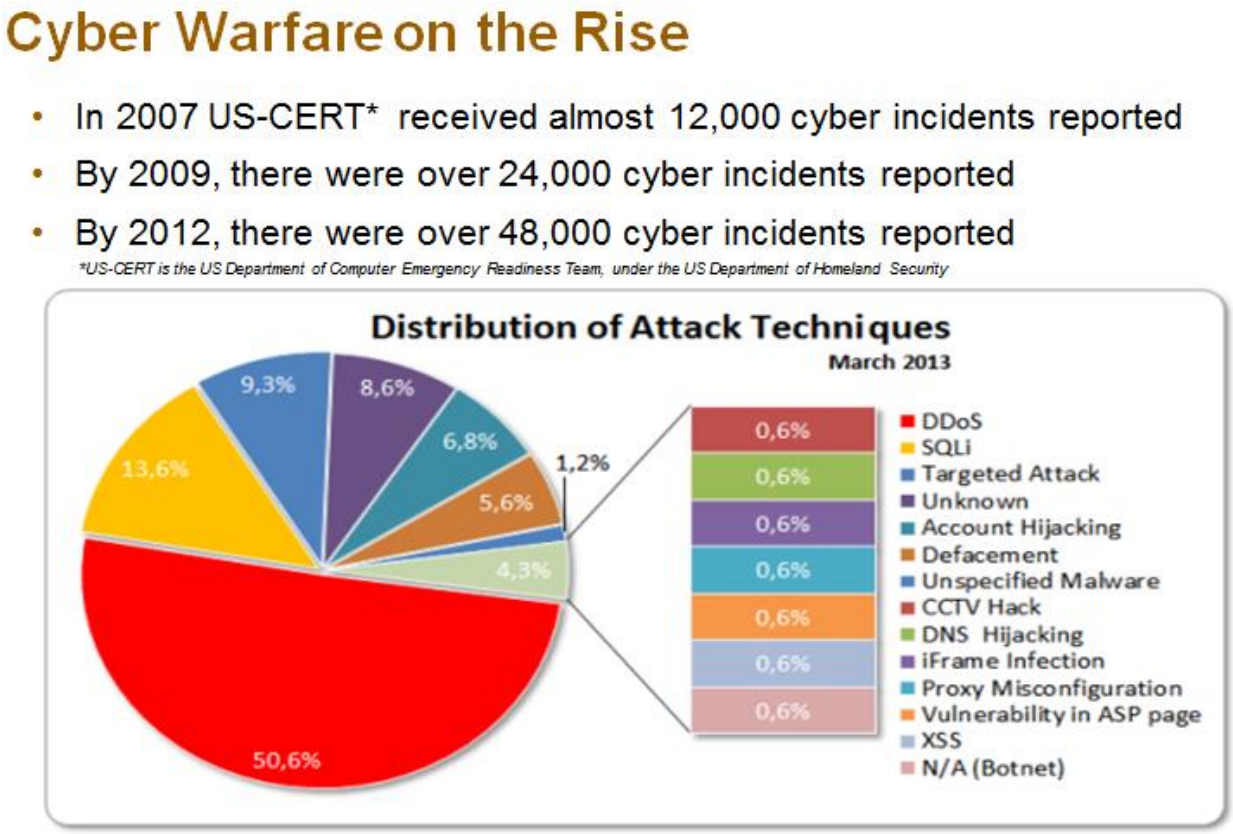
We're also seeing different motivations and actors behind DDoS Attacks. They have been used to attack oil field production systems by a Nation-State, directly impacting production. They have been used to target Financial Institutions to make their Internet presence unavailable. They have also been used as a "smokescreen" to disguise the real attack: steal data, or plant a foothold (backdoor) into vulnerable

systems for later use (and "persistent" presence). The motivations here are dependent upon the target and the "Cybercriminal," but the strategy is the same: identify the target, enumerate the vulnerabilities, develop and execute the game plan.

Finally, we shift our focus to the US Department of Computer Emergency Readiness Team, a division within the US Department of Homeland Security.

> ***"US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans. US-CERT's vision is to be a trusted global leader in cybersecurity – collaborative, agile, and responsive in a complex environment." (http://www.us-cert.gov/)***

US-CERT has a wealth of excellent resources and publications, which are very useful to better understand the threat landscape, and obtain guidance on specific countermeasures. So what is their perspective, on what we've dubbed the "Modern-Day Battlefield?"



Of course, "Cyber Incidents" is a bit of a loose term, and without delving into the nuances of this definition, let's instead examine the raw numbers. Within five years, there has been a dramatic increase in the number of incidents reported, and the types of attacks identified. More importantly, the vast majority of the Incidents have been classified as DDoS Attacks, with SQL Injection (SQLi) attacks in second place, and Targeted Attacks in third place.

This is an important correlation, because as we described above – DDoS Attacks are increasingly being used as a "smokescreen" to disguise the real attack, and SQL Injection is a tried and true technique to exploit Internet-facing systems. Here we can infer the same techniques: define the target, identify the vulnerabilities, develop the game plan, and then execute the attack strategy.

We've been talking about "increased sophistication" in tools and techniques used during attack campaigns. To dig a bit more deeply into this, we'll explore another objective set of data: The 2013 Verizon Data Breach Investigations Report. (http://www.verizonenterprise.com/DBIR/2013)

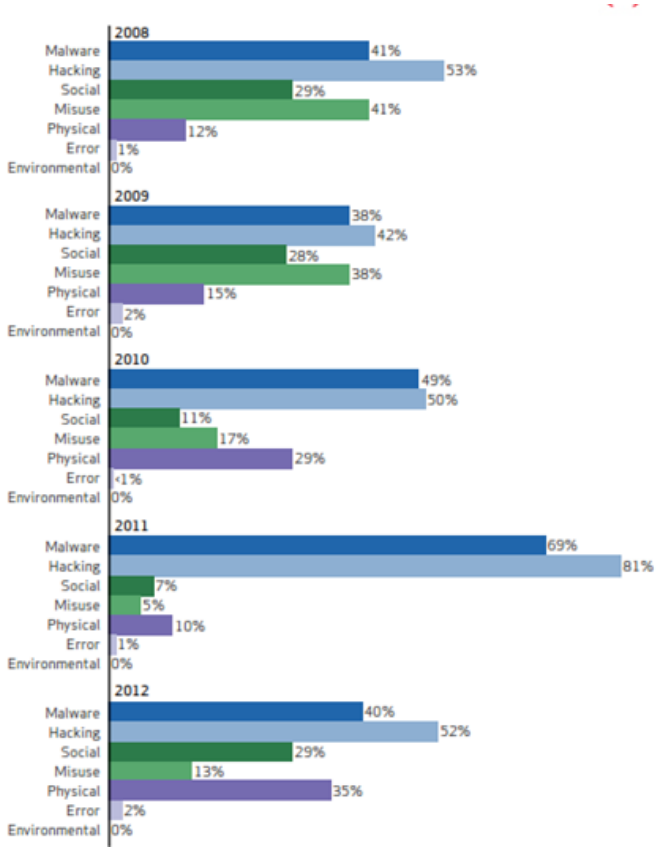
From their Investigations, based on real-world data breaches, they consistently find that Malware and Hacking are the chief methods by which data is compromised and stolen from organizations of all types. They have collaborated with many investigation and legal firms around the world, and so their dataset comprises a very clear perspective into "How" data breaches have occurred, and the most common methods employed. So we can be reasonably certain that with Malware and Hacking as the primary methods, a focus on how to defend against these types of attacks is important.

Classifying Breach Methods

- Notable Statistics:

1. Social Engineering is back on the rise after a 2 yr decline (spear phishing)
2. Malware and Hacking are consistent leaders
3. Physical attacks though on the rise are primarily tampering and POS attacks (discounting espionage for IP)
4. While Misuse seems to rise, it is likely skewed by sample and focused on financially motivated attacks

Source: Verizon 2013 Data Breach Investigations Report



Perhaps more important, however, is to again remind our audience that detection and response are still paramount. If you have an Internet presence, even if it's simply a website, it can be safely assumed that your systems will be routinely, regularly, and consistently probed for vulnerabilities. Both automated and manual efforts will be employed against your Internet-facing presence, either as a direct, intended

target, as collateral damage by association with other targets, or by simply having an Internet-facing IP address.

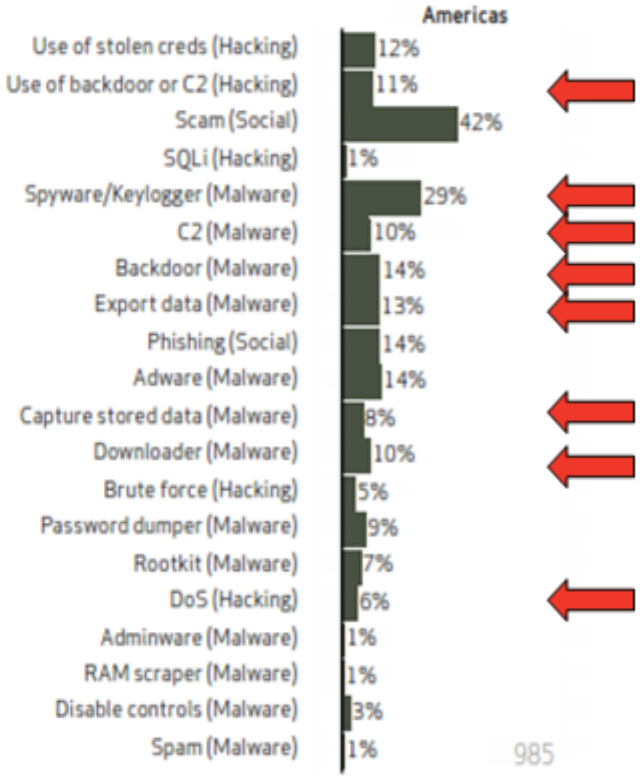
Malware comes in many forms and flavors, and the authors of malware continue to evolve the capabilities of the malicious software, to perhaps avoid detection, and surreptitiously insert itself into your systems. It can insert itself on your systems and wait for future commands, or be execution immediately with several different aims: plant backdoors ("footholds" and "beachheads"), destroy system and application capabilities, eavesdrop, and steal Data. By Data, we don't just mean the commonly perceived types of Data: Customer data, Financial Data, Intellectual Property, etc – although those are certainly part of the story. Indeed, by Data we also mean stealing credentials, including root Certificates. This is not the stuff of science fiction; this is the real deal, with very real motivations and sponsorship. Are you a target?

Finally, when we talk about "automated" attacks, we generally refer to Botnets. But keep in mind that Botnets are invoked as part of a campaign, an effort with intended consequences. They are created and initiated by people, and then run rampant when ordered to execute. Here again, Botnets are used for nefarious purposes, with all sorts of end-goals in mind, and based upon all sorts of motivations. We don't see an end to these in the near future, which is all the more reason to have a stronger detective and response capabilities.

Ask yourself: Can I see Botnet traffic directed at my infrastructure, or worse, such traffic leaving my infrastructure? Is it benign, 'normal Internet' traffic, or is there perhaps something else going on simultaneously?

Role of Botnets in Attacks

- Botnets are proliferating at a high rate.
- Botnets uses are expanding rapidly:
  - Theft of financial credentials
  - Self propagation
  - DDoS sourcing
  - Installation of keyloggers
  - Spam and Phishing sourcing
- Botnets are regularly updated and provide a Flexible platform for malware loading



Source: Verizon 2013 Data Breach Investigations Report

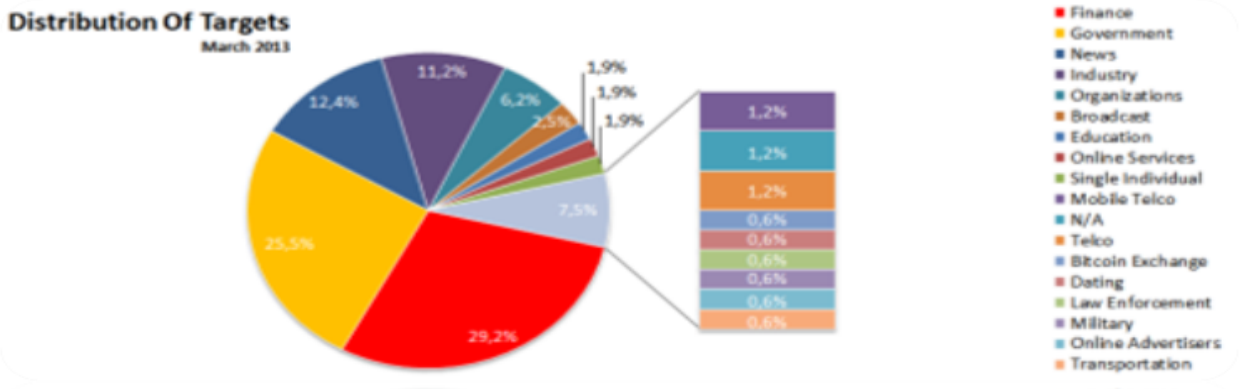
Finally, we wrap up the discussion with perspective to a pressing question: Are you a target? To answer that question, we suggest you ask yourself the following five questions:

1. Do you possess information that has direct financial value to a criminal (contract information, credit card or bank acount information, etc)?
2. Do you possess information that has indirect financial value to a criminal (sufficient data about individuals to commit identity theft, medical or criminal information that could be used for extortion, business impacting litigation information, etc)?
3. Do you possess intellectual property that might have value to offshore corporations or nation states (product designs, chemical or drug formulas, patents, unique processes, etc)?
4. Do you operate critical infrastructure that could be targeted to harm US citizens?
5. Has your organization ever done anything that might anger an individual or organization?

If you answered yes to any of the above, then you absolutely are a potential target.

Who is being Attacked?

- Biggest Target is Financial Services
- Second Biggest Target is Government
- News attacks are typically State Sponsored and Hacktivist
- Industry attacks are typically espionage targeting IP



Source: http://hackmageddon.com/2013/04/09/march-2013-cyber-attacks-statistics/

Is your agency at risk?

State Government:
South Carolina. The largest cyberattack against a state government put three-quarters of the state's population at risk for identity fraud. A hacker stole a database from the state's Department of Revenue, exposing 3.6 million Social Security numbers and 387,000 payment card records. More than 657,000 businesses also were compromised.

LAW ENFORCEMENT:
Man pleads guilty to attacks on Texas intelligence firms; also admits involvement in cyber attacks on law enforcement websites

Healthcare:
Utah health programs. Eastern European hackers pulled 780,000 Medicaid records from servers at Utah's Department of Technology Services. In addition to Medicaid patients, recipients of the state's Children's Health Insurance Program were affected, which makes this case particularly troubling.

UNIVERSITY SYSTEM:
School system, Tennessee. A hacker group calling itself SpexSec hijacked 110,000 records that included names, Social Security numbers and other personal information from the Clarksville-Montgomery County School System in mid-June. Current and former employees and students were affected."

Recent Examples:

http://www.washingtontimes.com/news/2011/nov/18/hackers-apparently-based-in-russia-attacked-a-publ/?page=all
http://www.upi.com/Top_News/US/2013/05/29/Anonymous-hacker-pleads-guilty-to-Austin-Texas-cyberattack/UPI-96691369830610/
http://www.signix.com/credit-union-news/bid/93563/Texas-credit-union-website-hit-by-cyber-attack
http://www.cyberwarnews.info/2013/04/01/first-national-bank-texas-hacked-social-security-details-leaked-for-opblacksummer/
http://otm.myfoxal.com/news/crime/157323-cybercrooks-use-interest-texas-plant-explosion-attack-computers
http://news.softpedia.com/news/Two-Journalism-Sites-of-the-University-of-Texas-at-Austin-Hit-by-Massive-Cyberattack-340277.shtml
http://www.esecurityplanet.com/network-security/texas-tech-university-health-sciences-center-admits-data-breach.html

[Type text]

Practical Guidance and Effective Countermeasures

It is safe to assume that you are, have been, or will be breached. Data will be compromised, data will be exfiltrated, and systems will be compromised. Without opening a very large can of worms, the concept of Advanced Persistent Threats clearly illustrates this. We can look no further than to the recent breaches of industry Stalwarts such as Bit9, Lockheed Martin, and RSA, to name just a few. It is quite safe to assume those organizations have very robust protective postures. The questions remain, however, around their effectiveness in detection and containment.

But these examples, regardless of the effectiveness of their ability to detect and contain, support our opinion that a singular focus on purely preventative controls is no longer effective on this modern-day battlefield. We opine the operating assumption is *that your systems and perimeter will be breached.* The more important consideration will be how effectively you can identify the breach – and how well you can contain it.

For this reason, we will always recommend a Third Party Assessment as an inclusive element of a comprehensive and effective Risk Management Program. Objective evaluation of your assumptions about your technical and procedural controls is critical to really understanding how well your "Security Spend" is matching your perceived risk posture. Risk is more than understanding vulnerabilities, technical tool sets, and exposures. Risk Management is defining how the three critical elements of any IT Organization function together, in order to provide maximum data and system protection: People, Processes, and Technology.

Third Party Assessments and expert consulting can help any organization, regardless of size, determine the most cost-efficient areas to focus upon for effective IT Risk Management. While the systems and approaches may seem complex, leveraging seasoned expertise, as opposed to the "lowest cost provider," will yield Valuable insight and guidance. From architecture and system design reviews, Data Discovery and Classification, Data Loss Prevention systems and processes, Access Control systems and processes, effective and comprehensive monitoring and Incident Response tools and processes, to Assessments and Penetration Testing – these complex concepts can best be designed and evaluated by *experienced* professionals.